CYBR 8950 Project Pitch
Adam Spanier

I. Title

Securing Distributed Control Systems using Novel Distributed Cryptographic Techniques

II. Problem

Programmable Logic Controllers (PLCs) are an essential component in distributed control systems (DCSs). PLCs are small hardware/software components that pair sensors with actuators via a small ladder logic software package to carry out physical operations in the real world. In DCS networks, PLCs are connected to centralized control software packages (DCSs) that coordinate, regulate, and maintain the sensor/actuation functionalities of the PLCs in the system.

PLCs are used because they are simple, cheap, and robust. Simplicity in PLCs makes them fast, efficient, and resistant to software flaws. As a result, the computing power they bring to bear is quite limited. When securing PLCs, very few additional security controls can be added to the native PLC hardware without negatively impacting the computational abilities of the device.

From the power grid to nuclear power plants, stop lights to water treatment plants, the most critical systems in the modern industrial world are run with PLCs. In fact, the notorious Stuxnet cyber attack is a result of a virus aimed at specific Siemens PLC configurations. Due to the weaknesses stated above, the attack was spectacularly successful, ushering in a new age of remote and devastating cyber attacks.

Current attempts to secure PLCs most often use Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), physical security protections, and external encryption mechanisms. While the combination of these systems does facilitate some system security, many DCS security systems end up being a disconnected patchwork of seemingly useful but disparate security controls lacking any real overarching security design.

While there is a wealth of PLC security research, this work aims to take a deeper look at novel, distributed cryptographic architectures and structures that could be combined with DCS designs to create a more holistic, system-wide approach to DCS security. This effort generates the following research question: **How can distributed cryptographic structures be combined, configured, and integrated into DCS designs to improve the security stance of the DCS network?**

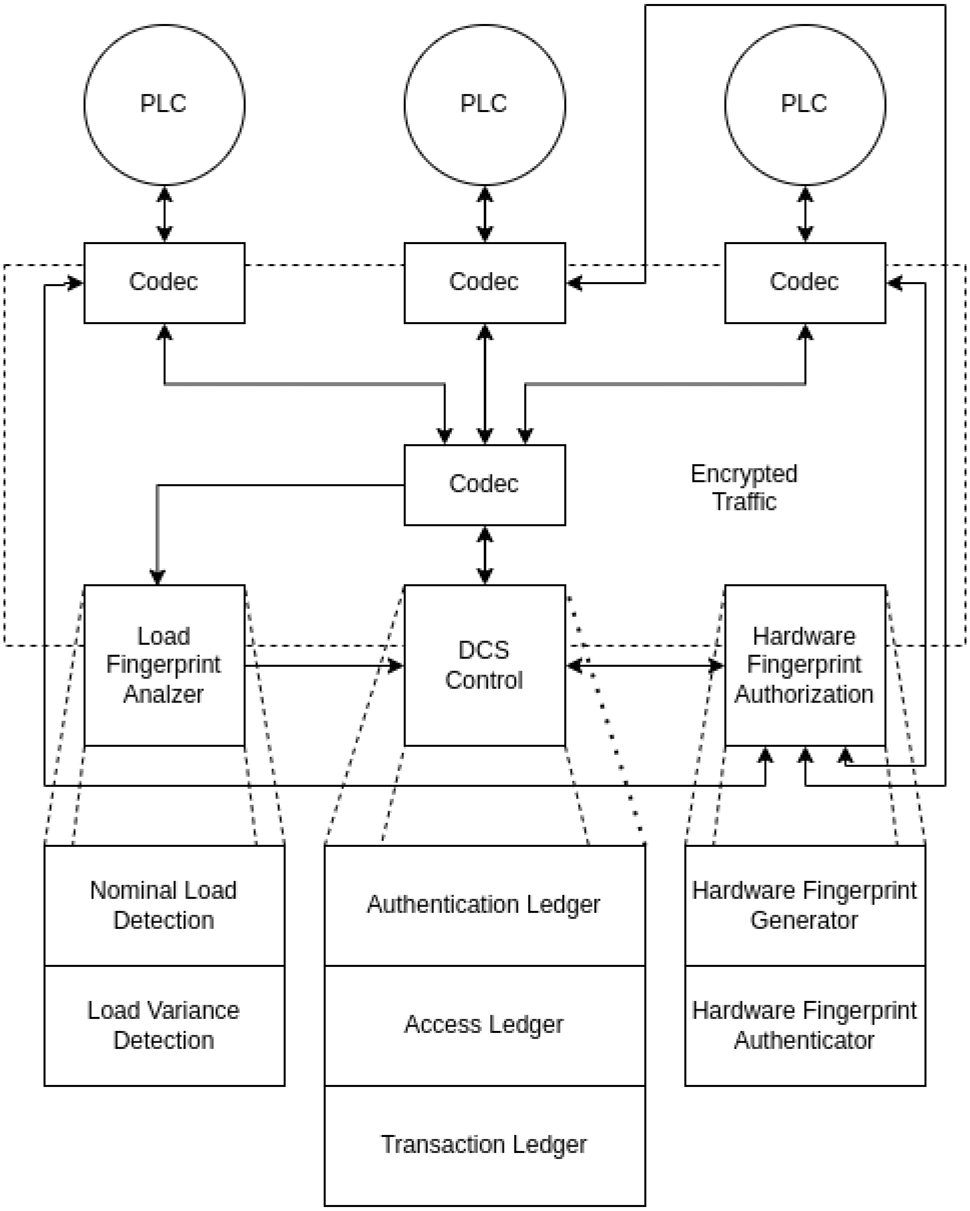
III. Scope

To find a solution to this problem, a literature review will be undertaken to gather needed context for what other researchers have already done in the area. Based on the literature review, a new system will be gleaned and subsequently designed form the efforts carried out in related works. This system will then be modeled, implemented, and prototyped in an effort to determine the validity of the solution. A discussion will be carried out on the findings of the work.

IV. Value Proposition

An attack on even a single critical DCS network like the US power grid would render the entire nation unable to carry on. All business transactions would halt, food production would cease, water would stop flowing, refrigerators would die, life support units would cease to function, toilets would stop flushing, computers would stop running, lights would stop shining, and numerous other essential systems would fail leading to untold amounts of human suffering. A more effective approach to DCS security not only provides stability for businesses, governments, and utilities, but also for every human life. To mitigate the probability of these events is to bolster public safety for all people.

V. Potential Diagram


PLC
PLC
PLC
Codec
Codec
Codec
Codec
Encrypted Traffic
Load Fingerprint Analzer
DCS Control
Hardware Fingerprint Authorization
Nominal Load Detection
Load Variance Detection
Authentication Ledger
Access Ledger
Transaction Ledger
Hardware Fingerprint Generator
Hardware Fingerprint Authenticator